Le Pentagone visé par une cyber-attaque russe ! | Le Net Expert Informatique

	Le Pentagone visé par une cyber-attaque russe !

Aux alentours du 25 juillet, des pirates informatiques russes ont lancé « une cyber-attaque sophistiquée » contre un système de courriels non confidentiels de l'état-major interarmées au Pentagone, selon des responsables américains ayant requis l'anonymat et cités par la chaîne NBC. Aucune fuite d'informations secrètes n'aurait eu lieu.

Le système informatique du Pentagone est débranché depuis une quinzaine de jours, l'attaque ayant visé 4 000 civils et militaires qui travaillent pour l'état-major interarmées, précise NBC.
Le Pentagone confirme avoir mis le système hors-circuit pour mener une enquête approfondie.
« Par principe et pour des raisons de sécurité opérationnelle, nous ne commentons pas les cyber-incidents ou attaques contre nos réseaux », a indiqué la lieutenant-colonel Valérie Henderson, l'une des porte-paroles du Pentagone dans un courriel.
Selon NBC, l'attaque était automatisée et a réussi, en moins d'une minute, à amasser et à rediffuser les informations collectées sur Internet. La cyber-attaque a été coordonnée par le biais de comptes cryptés et par les réseaux sociaux, d'après ces responsables américains anonymes. Le gouvernement russe n'a pas été directement accusé d'être à l'origine de l'attaque. Mais au regard de sa sophistication, l'attaque aurait été menée par des gens travaillant pour le compte d'une agence gouvernementale, précise NBC.
Ce n'est pas la première fois que des « hackers russes » mythiques sont accusés d'attaques contre les sites de médias et d'institutions occidentales. Fin avril dernier, le porte-parole du Kremlin, Dmitri Peskov, commentait les rapports sur les attaques de « pirates informatiques russes » contre les réseaux informatiques américains et estimait qu'accuser Moscou de tous les maux « était devenu une sorte de sport ».

Source : http://www.partiantisioniste.com/actualites/le-pentagone-vise-par-une-cyber-attaque-russe-2492.html

Alerte partagez – Nouvelle faille Android…| Le Net Expert Informatique

	Alerte partagez – Nouvelle faille Android…

En début de semaine l'affaire Stagefright révélait une faille majeure sur Android. Trend Micro en remet aujourd'hui une couche dévoilant une nouvelle faille critique. Non patchée par Google assure l'expert en sécurité.

Dure semaine pour Android. Trend Micro annonce la découvre d'une nouvelle faille qui cette fois permet de rendre le téléphone non fonctionnel. En début de semaine, l'affaire Stagefright avait déjà ébranlé l'aura de Google. Aucun correctif n'est encore disponible.
Quand cette faille est exploitée avec succès, le téléphone équipé d'Android devient silencieux. Plus d'alertes sur les messages, plus de sonnerie d'appel. Rien. Puis le téléphone se grippe, peu à peu, et s'arrête. La faille « est causée par un débordement d'entier lorsque le service de mediaserver analyse un fichier MKV. Il lit la mémoire de tampon ou écrit des données à l'adresse NULL lors de l'analyse des données audio » analyse Trend Micro.

Jelly Bean et Lollipop touchés
« La vulnérabilité réside dans le service mediaserver, qui est utilisé par Android pour les index de fichiers multimédias qui sont situés sur le périphérique Android. Ce service ne peut pas traiter correctement un fichier vidéo malformé utilisant le conteneur Matroska (généralement avec l'extension. mkv). Lorsque le processus ouvre un fichier MKV malformé, le service peut se bloquer (et avec lui, le reste du système d'exploitation) » explique Trend Micro.
Cette faille de sécurité peut être exploitée en incitant un internaute à visiter un site infecté, ou en lui faisant télécharger une application vérolée. Les versions d'Android impactées par cette faille courent d'Android 4.3 (Jelly Bean) à Android 5.1.1 (Lollipop).
Trend Micro a informé discrètement Google en mai dernier, mais l'entreprise n'aurait pas classé cette faille autrement qu'une «vulnérabilité de faible priorité », selon Trend Micro. Conséquence : aucun patch n'a été publié. Trend Micro prend donc aujourd'hui les devants et rend public cette faille, espérant que Google ait la même réactivité qu'avec Stagefright. Et Trend Micro en profite bien sûr pour faire la publicité de ses solutions, qui évidemment, protègent des complications de Google.

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.zdnet.fr/actualites/android-a-nouveau-victime-d-une-faille-39823130.htm

---

Attention aux arnaqueurs qui sévissent sur le site Immoweb

! | Le Net Expert Informatique

Attention aux arnaqueurs qui sévissent sur le site Immoweb !

Avec l'été, les fausses petites annonces pour des lieux de villégiature fleurissent sur les sites internet. Et dans quelques semaines, ce sera au tour des faux kots pour étudiants.

Le modus operandi des arnaqueurs est simple : on vous appâte avec un bien à louer à prix cassé. Puis, on vous demande une caution, à verser via un mandat postal ou Western Union. Et vous êtes quitte de votre argent… Immoweb tire la sonnette d'alarme. L'arnaque en question n'est pas nouvelle, mais elle a repris de plus belle avec l'arrivée des vacances scolaires. Pour l'instant, ce sont principalement des annonces pour des lieux de villégiature qui se révèlent fausses. « On peut ainsi voir une maison dans le sud de la France ou dans un lieu exotique, à un prix dérisoire », explique Olivier Bogaert, commissaire à la Computer Crime Unit, l'unité spécialisée dans la cybercriminalité de la police fédérale.
Le candidat locataire tombe sous le charme des photos alléchantes, et du prix cassé. Et il contacte via le site internet le propriétaire. Les discussions quittent alors l'espace du site internet où était placée l'annonce.
« Le propriétaire peut expliquer qu'il avait un locataire qui s'est désisté au dernier moment et qu'il baisse donc le prix, ou qu'il recherche surtout à ce que sa maison ou son appartement ne reste pas vide. Il est souvent à l'étranger, de sorte qu'il demande à ce que vous versiez un acompte ou le loyer via Western Union, ou via une banque étrangère. Il peut aussi demander à ce que vous lui envoyiez une carte de crédit prépayée, que vous aurez crédité d'un certain montant ».

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.
Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source :
http://www.sudinfo.be/1334805/article/2015-07-17/immoweb-prevent-ses-utilisateurs-attention-aux-arnaqueurs-qui-sevissent-sur-le

---

Ashley Madison tente de rassurer ses clients infidèles | Le Net Expert Informatique

12 Ashley Madison tente de rassurer ses clients infidèles

Alors qu'un maître-chanteur menace de diffuser un fichier de près de 40 millions d'hommes et de femmes inscrits sur Ashley Madison pour tromper leur conjoint, l'éditeur affirme qu'il a trouvé la parade : la loi américaine de protection du droit d'auteur.

Ce matin, nous rapportions que l'éditeur canadien du site de rencontres adultères Ashley Madison s'était fait pirater une base de données avec les noms de quelques 37 millions d'utilisateurs du service qui promet discrétion et anonymat. Alors qu'ils n'en ont publié que des extraits, les hackers promettent de publier l'intégralité de la base de données sur internet si la société Avid Life Media basée à Toronto ne ferme pas Ashley Madison et deux autres sites internet qu'elle édite.
Mais l'entreprise n'entend visiblement pas céder aux pressions et essaye de rassurer tant bien que faire se peut ses clients. Dans un communiqué envoyé à Numerama, Avid Life Media explique les contre-mesures mises en place, qui pourraient toutefois s'avérer vaines si les hackers décidaient de mettre leurs menaces à exécution et de passer par un réseau P2P incontrôlable comme BitTorrent pour publier la base de données intégrale. La société mise sur la loi américaine sur le droit d'auteur sur internet (le DMCA) qui impose aux plateformes de supprimer les contenus publiés sans l'autorisation des ayants droit lorsqu'elles sont notifiés. Elle estime que sa base de données est couverte par le DMCA.
Jusqu'à présent, les extraits des bases communiqués à titre de preuve du piratage ont effectivement été mis en ligne sur des sites de téléchargement direct qui acceptent de retirer les liens illicites qui leur sont notifiés, et qui l'ont fait. Mais ce ne sera pas le cas si les hackers (ou « le » hacker si l'on en croit les soupçons que porte l'entreprise sur un ancien collaborateur) décident, par exemple, de publier un simple fichier .torrent, comme l'ont fait récemment les pirates de Hacking Team. Il n'y a alors personne à qui envoyer une demande de DMCA, et/ou beaucoup de sites de liens BitTorrent qui ne les respectent pas.

Voici le communiqué reçu :
Suite à une intrusion injustifiée et criminelle dans notre système samedi 18 juillet 2015, Avid Life Media a immédiatement engagé l'une des équipes de sécurité informatique les plus pointues au monde afin de prendre toutes les mesures possibles pour résoudre cette crise.
En utilisant la Digital Millennium Copyright Act (DMCA), notre équipe a supprimé avec succès tous les messages liés à cet incident ainsi que toutes les Informations Personnelles Identifiables (PII) publiées en ligne à propos de nos utilisateurs.
La confidentialité des informations concernant nos utilisateurs a toujours été notre plus grande priorité, et nous sommes rassurés que les dispositions contenues dans le DMCA aient permis de résoudre ce problème efficacement. Notre équipe de spécialistes et de professionnels sécurité informatique, en plus de faire appliquer la loi, continuent d'enquêter sur cet incident, et nous publierons de futurs bulletins dès que de nouveaux éléments verront le jour.

Source : http://www.numerama.com/magazine/33730-quand-ashley-madison-tente-de-rassurer-ses-clients-infideles.html
Par Guillaume Champeau

Le site de rencontre Madison Ashley piraté – l'analyse de Kaspersky Lab | Le Net Expert Informatique

Le site de rencontre Madison Ashley piraté – l'analyse de Kaspersky Lab

Le site de rencontres adultères canadien Ashley Madison, qui revendique plus de 37 millions d'inscrits, a été victime d'une attaque informatique ayant pour but de voler les données personnelles d'un grand nombre d'utilisateurs. Ces données ont été brièvement mises en ligne.

Marta Janus, chercheuse en sécurité au sein de l'équipe de recherche et d'analyse (GReAT) du spécialiste en sécurité Kaspersky Lab, revient sur cette attaque :
Marta Janus « L'attaque subie par Madison Ashley nous rappelle à quel point il est important pour toutes les entreprises de mettre en place des mesures de sécurité contre les cyberattaques, afin de protéger les données personnelles de leurs utilisateurs. Un internaute qui accepte de confier certaines de ses données privées à un site web devrait être assuré que ses informations seront conservées de la façon la plus sécurisée qui soit, et les entreprises concernées devraient pouvoir s'y engager.
Il faut également rappeler que toutes les failles de sécurité qui entrainent des fuites de données privées sont un problème, quelles que soit la nature du site visé, sa moralité et même sa légalité. Dans le cas de l'attaque contre Ashley Madison, l'affaire est très sérieuse car la fuite concerne des informations comme les noms, les adresses ou encore les données bancaires. Une fois rendues publiques, ces informations pourraient par exemple être utilisées pour voler de l'argent.
Les raisons pour lesquelles une entreprise peut être victime d'une cyber attaque sont nombreuses – argent, politique ou même éthique. N'importe quelle entreprise peut être la cible d'une attaque et même si les solutions de sécurité réduisent les risques que cette attaque soit fructueuse pour les criminels, d'autres mesures existent pour une protection renforcée. Je pense notamment aux mises à jour logicielles, encore trop souvent remises au lendemain, à la réalisation régulière d'audits de sécurité ou encore au test des infrastructures. Le meilleur moyen de lutter contre ce type de cyberattaques est de se protéger avant qu'elles ne frappent en disposant d'une stratégie de sécurité complète et efficace. »

Source : https://www.globalsecuritymag.fr/Site-de-rencontre-pirate-l-analyse,20150720,54540.html
par Kaspersky Lab

Alerte partagez ! Deux nouvelles failles zero-day dans le plugin Flash d’Adobe | Programmez! | Le Net Expert Informatique

	Alerte partagez ! Deux nouvelles failles zero-day dans le plugin Flash d’Adobe

Il y en a des choses intéressantes dans les 400 Go de données récemment dérobées à la société The Hacking Team et publiées sur Pastebin

The Hacking Team est une société qui vit du cyber espionnage, mais qui en l'occurrence contribue pour le moment et à l'insu de son plein gré à la sécurité informatique. En effet le code source de son logiciel espion phare, DaVinci, fait partie des 400 Go volés. Et ce code source est riche d'enseignements.
Ainsi, il est apparu en fin de semaine dernière que DaVinci exploitait une faille zero-day dans le plugin Flash d'Adobe. Faille qu'Adobe a d'ailleurs rapidement corrigée.
Mais ce n'est pas tout. Après cette faille CVE-2015-5119, deux autres failles zero-day ont été identifiées grâce à The Hacking Team CVE-2015-5122 et CVE-2015-512 respectivement. Des failles dans le plugin Flash, encore et toujours… FireEye et Trend Micro détaillent quelques informations techniques à propos de ces failles, sur les pages citées.
Dans les deux cas, les failles consistent en des corruptions mémoire, dont l'exploit rend possible l'exécution d'un code arbitraire sur la machine attaquée. Il s'agit donc de failles hautement critiques, qui pour l'instant ne sont pas corrigées. En attendant les correctifs, les experts en sécurité recommandent très vivement la désactivation du plugin Flash, en raison de la gravité de ces failles.
Lire la suite….

Source : http://www.programmez.com/actualites/hacking-hacking-team-deux-nouvelles-failles-zero-day-dans-le-plugin-flash-dadobe-23012

Les dessous de la société d'espionnage Hacking Team… | Le Net Expert Informatique

Les dessous de la société d'espionnage Hacking Team…

La firme, qui s'est fait voler plus de 400 gigaoctets de données confidentielles, avait présenté ses technologies aux services de renseignements français. La société Hacking Team, soupçonnée d'avoir livré des logiciels d'espionnage à des régimes autoritaires, assure n'avoir rien commis d'illégal.

On soupçonnait Hacking Team de rouler sa bosse pour des dictatures. Et voilà que le journal Le Monde nous apprend que la sulfureuse entreprise d'espionnage a également eu des contacts avec les services d'espionnage français… Lundi 6 juillet, la société italienne a été victime d'un piratage de grande ampleur de ses données confidentielles et des comptes Twitter de plusieurs de ses responsables. Des centaines de gigaoctets de données se sont déversées sur le Web et ont été immédiatement téléchargées et consultées par ceux qui l'accusaient de faire bénéficier de ses technologies des régimes autoritaires.
L'entreprise est en effet spécialisée dans le développement et la commercialisation de logiciels de surveillance ou de piratage très performants, principalement destinés à des États. Logiciels de blocage de pages internet, systèmes de mise sous surveillance de boîtes mails jugées suspectes… Hacking Team a développé une impressionnante gamme de services. Leur produit phare, dénommé RCS (pour Remote Control Systems), est un packaging incluant des logiciels tels que DaVinci et Galileo, qui permettent de visualiser les frappes effectuées sur le clavier de l'ordinateur visé, d'en collecter les informations sensibles telles que les adresses mails, les documents enregistrés ou les mots de passe, ou encore de récupérer les historiques de navigation.

Ennemie d'Internet
La facilité avec laquelle ces outils peuvent être utilisés à des fins d'espionnage de masse avait conduit certaines ONG à dénoncer les pratiques de cette société. Cette dernière avait même fini par être classée parmi les ennemis d'Internet par Reporters sans frontières en 2013, en raison des rapports commerciaux qu'elle entretenait alors avec le Maroc et les Émirats arabes unis. Des traces de ses logiciels avaient ainsi été retrouvées sur les ordinateurs du site d'information marocain Mamfakinch, quelques jours après que ce média a reçu le Breaking Borders Award 2012 remis par Global Voices et Google.
Autre soupçon : « Un expert en sécurité, Morgan Marquis-Boire, a examiné des pièces jointes attachées à un e-mail envoyé à Ahmed Mansoor, un blogueur émirati. Elles étaient contaminées. Il y a trouvé de fortes indications suggérant que la source du cheval de Troie provenait de Hacking Team », écrit également RSF.
L'entreprise jouit dans le milieu d'une réputation douteuse, et est soupçonnée de collaborer avec des pays peu recommandables. Jusqu'à présent, la société clamait son innocence et aucune preuve de son implication dans la mise en place des systèmes de surveillance électronique de ces pays n'avait été découverte. « Nous faisons extrêmement attention à qui nous vendons nos produits. Nos investisseurs ont mis en place un comité légal qui nous conseille continuellement sur le statut de chaque pays avec lequel nous entrons en contact », assurait le PDG de Hacking Team, David Vincenzetti, dans une interview accordée en 2011 au journaliste Ryan Gallagher.

Des régimes autoritaires en clients
Kazakhstan, Arabie saoudite, Azerbaïdjan… De nombreux États – dont les dirigeants ne font pas toujours des libertés individuelles une priorité de leur règne… – font partie de la liste des clients. Parmi ces pays, certains sont connus pour une répression dure de leur population et leurs violations répétées des droits de l'homme. On peut ainsi noter l'exemple du Soudan, avec lequel Hacking Team a toujours nié avoir collaboré. Cependant, les documents publiés révèlent l'existence d'un contrat de 480 000 euros avec le gouvernement actuellement en place. La Russie fait également partie des heureux bénéficiaires des services de Hacking Team. La firme prend même la peine d'indiquer sur ses documents internes que ces deux pays ne sont « officiellement pas clients » (« officially not supported ») de l'entreprise.
Interrogé au sujet de la série de contrats signés avec le Soudan, le porte-parole de l'entreprise, Éric Rabe, a quant à lui maintenu que le document cité remontait à avant les sanctions décidées par les Nations unies contre le pays.

La France, elle aussi intéressée par les services de l'entreprise
D'après certains documents, la France et Hacking Team seraient entrés en contact plusieurs fois ces dernières années. La prise de contact entre le ministère de la Défense et l'entreprise a eu lieu en 2013, alors qu'une réunion de présentation s'est tenue fin 2014 dans un hôtel près de l'aéroport Charles-de-Gaulle à Paris. Étaient représentés à cette réunion la DGSI et le Groupement interministériel de contrôle (GIC) chargé quant à lui des écoutes administratives (c'est-à-dire menées sans mandat judiciaire), et dirigé par le Premier ministre.
Si la DGSI affirme n'avoir donné aucune suite à cette réunion, ce n'est pas le cas du GIC qui a poursuivi ses échanges avec Hacking Team. Comme le révèle un échange de courriels entre le GIC et Hacking Team, Philippe Vinci, l'un des responsables de l'entreprise, s'est rendu au siège du GIC le vendredi 3 avril 2015. Cette information est confirmée par un échange de courriels entre la société et le groupement interministériel datant du mardi 7 avril. On y apprend également que le GIC serait intéressé par une démonstration de la part d'Hacking Team. L'entreprise aurait alors proposé aux représentants du GIC de venir assister à une telle démonstration en Italie courant mai. Aucune information concernant la suite à donner à ces rendez-vous n'a pour le moment fuité.

« Nous n'avons rien à cacher »
Après deux jours sans réaction, l'entreprise a finalement commenté ce vol de données dans une interview accordée au site IBTimes : « Nous n'avons rien à cacher sur nos activités et nous pensons qu'il n'y a aucune preuve dans ces 400 gigabits de données que nous avons violé une quelconque loi », a ainsi affirmé le porte-parole de l'entreprise, Éric Rabe.
Pour le moment, et en attendant de connaître exactement le contenu des données qui ont été piratées, la société italienne a demandé à ses clients de cesser d'utiliser ses logiciels. Les auteurs du piratage ne se sont pas encore manifestés.

Source : http://www.lepoint.fr/high-tech-internet/les-curieux-clients-de-la-societe-d-espionnage-hacking-team-08-07-2015-1943190_47.php
Par Ian BEAURAIN

Des hackers paralysent l'aéroport de Varsovie pendant cinq heures | Le Net Expert Informatique

Des hackers paralysent l'aéroport de Varsovie pendant cinq heures

Une attaque contre les systèmes informatiques de la compagnie aérienne polonaise LOT a cloué au sol dimanche 1400 passagers pendant plus de cinq heures à l'aéroport Chopin de Varsovie. Une dizaine de vols intérieurs et internationaux ont été annulés.

L'attaque a eu lieu vers 17 heures (en Suisse). Le système informatique visé régit le plan des vols de la compagnie, sans lequel aucun décollage ne peut se faire. Le problème a été maîtrisé vers 22 heures, a annoncé LOT.
Le trafic aérien a repris en fin de soirée. « Il s'agit d'une première attaque de ce genre (contre LOT, ndlr). Il y a eu dans le passé des attaques contre d'autres compagnies aériennes », a déclaré un porte-parole de la compagnie.
« Ces attaques ont des effets pénibles et très spectaculaires », a-t-il ajouté, en déplorant les inconvénients causés aux passagers. Il a assuré qu'ils avaient reçu l'aide nécessaire, y compris la possibilité de passer la nuit dans des hôtels à Varsovie.
Les services de sécurité polonais, notamment l'agence de sécurité intérieure ABW et le centre gouvernemental de sécurité, ont été mobilisés.

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.
Besoin d'informations complémentaires ?
Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.
Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.lacote.ch/fr/monde/cybercriminalite-des-hackers-paralysent-l-aeroport-de-varsovie-pendant-cinq-heures-481-1476594
Source : ATS

Alerte ! Campagne de pourriels avec documents Microsoft Office malveillants | Le Net Expert Informatique

Alerte ! Campagne de pourriels avec documents Microsoft Office malveillants

Le CERT-FR alerte sur des pourriels qui se diffusent depuis une semaine en dépit des filtres antispam : attention aux macros malveillantes qu'ils diffusent !

Depuis une semaine, il est observé à l'échelle nationale une vague de pourriels dont le taux de blocage par les passerelles antispam est relativement faible.
Ces pourriels embarquent des documents Microsoft Office contenant des macros VBA malveillantes. Ces macros ont pour but d'infecter la victime avec Dridex, qui est un logiciel malveillant de type bancaire.
Selon les échantillons, le téléchargement de Dridex peut être effectué de deux façons différentes :
• la macro VBA télécharge puis exécute un script à partir du site pastebin.com. Ce dernier télécharge ensuite le binaire Dridex à partir d'un serveur malveillant ;
la macro VBA télécharge directement le binaire Dridex à partir d'un serveur malveillant.

Il est intéressant de noter que ces pourriels sont très souvent rédigés dans un français sans faute. Le sujet et le contenu du pourriel mentionnent des problèmes de facturation, dans la plupart des cas, pour inciter la victime à ouvrir la pièce jointe.

Le format utilisé dans cette campagne pour les documents malveillants est peu rencontré. En effet, si l'on connaît déjà bien les formats OLE et OpenXML, deux autres formats moins connus commencent à être de plus en plus utilisés pour la propagation de contenu malveillant. Il s'agit du format XML, déjà mentionné dans le bulletin d'actualité CERTFR-2015-ACT-017, et du format MIME HTML qui est le format utilisé dans cette campagne. Ces deux derniers formats ont l'avantage pour les attaquants d'être souvent moins bien détectés par les antivirus.
Bien sûr, les techniques classiques d'obfuscation du code VBA, telles que celles décrites dans le bulletin d'actualité précédemment mentionné, sont toujours utilisées.
A travers les échantillons qui ont pu nous être remontés, le CERT-FR a pu observer les URLs de téléchargement via pastebin suivantes (toutes les URLs suivantes ont été démilitarisées par l'adjonction du suffixe _BAD_ aux noms de domaines et adresses IP) :
http://pastebin.com._BAD_/download.php?i=2YzPHtum
http://pastebin.com._BAD_/download.php?i=wLeUenhF
http://pastebin.com._BAD_/download.php?i=umCDngcn
Pour les documents dont la macro VBA télécharge directement Dridex, le CERT-FR a pu observer les URLs de téléchargement suivantes :
http://www.adriatic-stone.hr._BAD_/64/11.exe
http://gb0004424.ferozo.com._BAD_/25/10.exe
Enfin, les échantillons Dridex ainsi récupérés tentent de communiquer avec les serveurs suivants :
https://94.23.53.23._BAD_:2443/
https://176.99.6.10._BAD_:8443/
https://173.230.130.172._BAD_:2443/
https://203.151.94.120._BAD_:4443/
https://31.186.99.250._BAD_:8443/
https://146.185.99.250._BAD_:8443/
https://185.12.95.40._BAD_:7443/
https://50.63.174.16._BAD_:6443/
https://79.143.191.147._BAD_:6443/
https://37.143.9.63._BAD_:4433/
Afin de se protéger contre ce type de menace, les conseils habituels sont rappelés :
ne pas ouvrir les documents ou les pièces jointes non sollicités ;
désactiver l'exécution automatique des macros dans les suites bureautiques ;
maintenir le système d'exploitation et l'anti-virus à jour.
La désactivation de l'exécution automatique des macros se paramètre dans le menu suivant :
Fichier / Options / Centre de gestion de la confidentialité / Paramètre du Centre de gestion de la confidentialité / Paramètres des macros / Désactiver toutes les macros avec notifications
Documentation
Recrudescence des attaques par macro « Visual Basic for Applications » dans les documents Microsoft Office – Bulletin d'actualité CERTFR-2015-ACT-017 :
http://www.cert.ssi.gouv.fr/site/CERTFR-2015-ACT-017/index.html
CVE-2012-0158 exploit evades AV in Mime HTML format :
http://blog.malwaretracker.com/2013/08/cve-2012-0158-exploit-evades-av-in-mime.html5
3

Afin de se protéger contre ce type de menace, les conseils habituels sont rappelés :
• ne pas ouvrir les documents ou les pièces jointes non sollicités ;
• désactiver l'exécution automatique des macros dans les suites bureautiques ;
• maintenir le système d'exploitation et l'antivirus à jour.

Le bulletin d'actualité du CERT-FR détaille les formats de documents et techniques utilisées ainsi que les parades à mettre en place.
Note :
*VBA : Visual Basic for Application est une implémentation de Microsoft Visual Basic intégrée dans l'ensemble des applications de Microsoft Office.

Pour aller plus loin :
Consulter les bulletins d'actualité sur le site du CERT-FR, le bulletin du 15 juin à : http://www.cert.ssi.gouv.fr/site/CERTFR-2015-ACT-024/index.html

---

Source : http://www.ssi.gouv.fr/actualite/campagne-de-pourriels-avec-documents-microsoft-office-malveillants/
Par l'ANSSI

Kaspersky annonce être victime d'une Cyberattaque | Le Net Expert Informatique

Kaspersky annonce être victime d'une Cyberattaque

L'éditeur de sécurité indique qu'une cyber-attaque a ciblé ses propres installations par le biais d'une nouvelle version du malware baptisé Duqu. Pour Eugene Kaspersky, le patron et fondateur de la société, cette offensive a pu être soutenue par un Etat.

Eugene Kaspersky prend la parole pour livrer les détails de l'attaque qui a visé les installations de l'éditeur de sécurité. Au cours d'une conférence de presse, le fondateur de la société a indiqué que les pirates ont utilisé une nouvelle variante d'un ver baptisé Duqu. Selon le patron de l'éditeur russe, le malware a été développé par une organisation très qualifiée, possiblement soutenue par un gouvernement étranger.
Eugene Kaspersky indique que ses équipes sont actuellement en train de rassembler l'ensemble des éléments pour comprendre l'attaque. Le responsable se veut toutefois rassurant. « Cette attaque n'a rien compromis pour nos clients mais également nos partenaires. Nous ne disposons pas encore de toutes les informations sur cette attaque mais je lance un avertissement clair, ne me hackez pas, c'est une mauvaise idée ».
L'éditeur s'est rendu compte de l'attaque grâce à une version Alpha de sa nouvelle solution censée lutter contre les menaces dites persistantes (ou APT pour advanced persistent threat). Pour Kaspersky le but des pirates était d'ailleurs d'espionner sa technologie permettant de traquer ce type de cyber-attaques.
Selon les spécialistes, Duqu est une variante de Stuxnet, un élément malveillant qui avait été utilisé pour attaquer des systèmes critiques dits SCADA. Stuxnet avait même permis d'organiser une cyber-attaque contre des installations informatiques présentes au sein d'une centrale nucléaire en Iran.
Toujours est-il qu'Eugene Kaspersky considère que le nouveau Duqu exploite plusieurs vulnérabilités 0-Day. Le fait d'être en mesure d'utiliser plusieurs failles jusqu'à présent inconnues est, selon le responsable, un élément important. Cela lui permet d'affirmer que les équipes derrière ce malware disposent non seulement de très solides connaissances techniques, mais également de soutiens « officiels » d'un gouvernement étranger.

Duqu, une nouvelle variante
Le malware Duqu avait déjà sévi en 2011. Mis en lumière par les équipes de Symantec, il était parvenu à se diffuser par le biais d'un fichier d'installation contenu dans un document Word (.doc) envoyé par e-mail. Une fois ouvert, ledit fichier exploitait une vulnérabilité du moteur d'analyse de font (TTF) Win32k TrueType et était ainsi capable d'infecter un poste informatique.
Microsoft avait par la suite été obligé de publier un patch de sécurité hors-cycle pour corriger les nouvelles vulnérabilités (0-Day) exploitées par le ver. A présent qu'une nouvelle variante du malware est détectée, la firme américaine pourrait à nouveau publier une mise à jour de sécurité pour l'ensemble de ses services.

Source : http://pro.clubic.com/it-business/securite-et-donnees/actualite-769814-kaspersky.html
Par Olivier Robillart